ESTABLISHING A CYBER WARRIOR FORCE

GRADUATE RESEARCH PROJECT

Scott D. Tobin, Major, USAF

AFIT/GE/ENG/04-27

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this graduate research project are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

AFIT/GE/ENG/04-27

ESTABLISHING A CYBER WARRIOR FORCE

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical & Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Electrical Science

Scott D. Tobin, BS, MA

Major, USAF

September 2004

AFIT/GE/ENG/04-27

ESTABLISHING A CYBER WARRIOR FORCE

Scott D. Tobin, BS, MA

Major, USAF

Approved:

/SIGNED/	7 Sep 04
Richard A. Raines, PhD, USAF (Chairman)	Date
/SIGNED/	7 Sep 04
Rusty O. Baldwin, PhD, USAF (Member)	Date
/SIGNED/	7 Sep 04
Robert F. Mills, PhD, USAF (Member)	Date

AFIT/GE/ENG/04-27

To my family and closest friend who endured this year along with me

Acknowledgments

I would like to express my sincere appreciation to my faculty advisor, Dr. Rick Raines for his guidance and support throughout the course of this research effort. It was his motivation that identified this topic for my research, and it proved to be very enlightening. I would also like to thank the numerous professionals across the Air Force, some old colleagues and some new acquaintances, who took the time from their busy days to field my questions and provide their wisdom and expertise. Without their assistance, I couldn't have completed this effort.

Scott D. Tobin

AFIT/GE/ENG/04-27

Abstract

Cyber Warfare is widely touted to be the next generation of warfare. As America's reliance on automated systems and information technology increases, so too does the potential vulnerability to cyber attack. Nation and non-nation states are developing the capability to wage cyber warfare. Historically, the Air Force and DoD have concentrated their efforts toward defensive network operations. However, a shift in doctrine has shown both the Air Force and DoD acknowledging the potential for Information Warfare. What appears to be lacking is the trained and educated cyber warrior force that will carry out the information operations if needed. This research project examines the doctrine of DoD and national agencies to engage in information operations and efforts in place to train cyber warriors. In turn, this research project offers recommendations for a career development and progression model for an Air Force *Cyber Warrior* force.

Table of Contents

Page

List of Figures

Page

List of Tables

Page

AFIT/GE/ENG/04-27

ESTABLISHING A CYBER WARRIOR FORCE

I. Introduction

Background

Information warfare (IW) is real. The threat is real. The potential for conflict centered around IW appears real.

> The competition for information is as old as human conflict. It is virtually a defining characteristic of humanity. Nations, corporations, and individuals each seek to increase and protect their own store of information while trying to limit and penetrate the adversary's…As information systems permeate our military and civilian lives, we are crossing a new frontier - the Information Age. It will define the 21st century and influence all we do as an air force. Information Warfare has become central to the way nations fight wars, and will be critical to Air Force operations in the 21st century. [1]

These viewpoints were taken from Cornerstones of Information Warfare, dated 1995. Nearly ten years ago, Air Force leadership recognized the future trend toward IW. Even the current Air Force Chief of Staff, General John Jumper, sees IW as an integral part of Air Force operations. "I picture myself around that same targeting table where you have the fighter pilot, the bomber pilot, the special operations people and the information warriors. As you go down the target list, each one takes a turn raising his or her hand saying, I can take that target" [2]. Will America ever see an actual information war? Who knows…these key military leaders certainly appear to think it's a real possibility and one the Air Force needs to prepare for. But what exactly is IW? According to the USAF Concept of Operations (CONOPS) for Information Operations

(IO), IW is defined as, “The theory of warfare in the information environment that guides the application of information operations to produce specific battlespace effects in support of commander’s objectives” [3]. A more broad definition however, comes from Dr Ivan Goldberg, researcher of information warfare, who says

> Information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries. [4]

Vulnerabilities

But why has information warfare become such a threat? Possibly because of the value of information as stated above. It may also be due to the fact that America is so dependent on information that it makes us vulnerable to attack. In 1998, it was estimated that 62 million Americans used the Internet to communicate, bank, shop, and do business [5]. And today there are over 200 million Americans on-line [6]. And not only are civilians vulnerable to IW due to their heavy reliance upon information and information systems, but the United States has a technologically advanced military who are also very *connected*. That dependence however, also leaves us vulnerable as well. “…a combination of cost concerns and the superiority of established commercial systems have created a situation in which an estimated 95 percent of all military communications travel over commercial systems” [7]. So not only is the average American susceptible to an information attack, but so is the military.

Threats

So is IW the only real threat? That's probably a difficult question to answer absolutely, however there are several authorities who feel it would be difficult to match the United State's and their allies' military might.

> Without doubt, the United States is the primary superpower in the world today. The end of the Cold War, the collapse of the Soviet Union, and the coalition victory in Iraq have all demonstrated the military dominance of U.S. forces. Despite substantial forces reductions in recent years, the United States and the Western European Allies will likely remain the most powerful military powers in the world for the near future. [8]

A common theory among many military leaders and strategists is that China is the only remaining serious military threat to the US. However, according to a recent Pentagon report [9], there's even speculation as to whether or not their military might is capable of matching ours. The report stated, "…China's leaders believe their military forces are not yet strong enough to compete directly with the American military." Consequently, China has embarked on a new strategy they think may help level the playing field. Specifically, "the concept appears to include a range of weapon systems and technologies related to information warfare…" which makes the threat of IW even more real. From that, one could easily conclude there's little threat of conventional war against the United States. Unfortunately however, that means the threat of asymmetrical warfare, in particular information warfare, remains real. According to the U.S. Army's *Doctrine for Asymmetric Warfare*, "…asymmetric warfare deals with unknowns, with surprise in terms of ends, ways, and means. The more dissimilar the opponent, the more difficult it is to anticipate his actions..." [10]. And with America's heavy dependence on

information and technology, IW becomes a very logical means for an adversary to exploit that dependence.

Not only are nation-states like China actively pursuing the cyber domain and the potential it offers, but information attacks and the ease with which they can be carried out appear to be of great interest to terrorist organizations as well. Al Qaeda is said to be engaged in the information warfare arena. Richard Clarke, former Special Adviser for Cyberspace Security, said of Al Qaeda, "…these people are gathering skills in cyber war capability…I think it suggests that someday we may see Al Qaeda, if it's still alive and operating, use cyberspace as a vehicle for attacking infrastructure -- not with bombs, but with bytes" [11]. And he's not alone in his opinion. Analysts with iDefense, purportedly the nation's only independent cyber intelligence company, claim Malaysia is one of the newest breeding grounds for cyber terrorists with the United States being one of their primary targets [12].

This information tends to support the theory that IW is a distinct possibility. Several senior military leaders clearly stated their beliefs that IW is the way wars will be fought in the future, the question is, are we ready? This research project examines that question. It looks at how the Air Force and DoD have shifted their doctrine from a defensive posture to one which includes offensive information operations. This project examines how several Air Force career fields train and qualify their individuals and uses key elements of those processes to recommend a career development and progression model for an Air Force *Cyber Warrior* force.

II. Current Situation

Defensive Posture

So how prepared is the United States and its military to defend against an information warfare attack? Much of that is up for speculation, but clearly based on comments from past and present Air Force leadership, they've had IW in their crosshairs for the last decade. However, considering efforts dealing with military network operations, they have focused primarily on the defensive aspects of network operations, labeled NetD, for network defense [13]. Several years ago, the Air Force realized the significance of the cyber threat that exists and took proactive steps to address it. In 1997, Air Force leaders conceived the notion of a new philosophy toward their networks and information systems. In January 1998, they formalized that notion and established a program entitled Operationalizing and Professionalizing the Network (OPTN) in order to apply the same operational rigor toward Air Force networks that the Air Force uses with weapons systems. OPTN established a structured, hierarchical management system with operations centers at the base, major command, and Air Force levels. It offered a structured training and equipping philosophy in an attempt to follow the lead of weapons systems. OPTN also adopted mainstream operational reporting of Air Force network statuses and graduated response measures in the event of an information attack. Although the focus was heavily process-oriented, it began to address the key concerns Air Force leadership had toward defending Air Force networks from outside attacks [14]. In 1998, then Air Force Chief of Staff, General Mike Ryan, articulated this even more clearly in a memorandum which stated "We continue to experience incidents on our networks which reinforce the need for improved network protection." He went on to

direct actions to install defensive network monitoring tools and procedures to improve the security of Air Force networks [15]. The Department of Defense (DoD) made an even louder statement about the importance of network security that year when they activated a new joint service operations center to manage military networks called the Joint Task Force (JTF) for Computer Network Defense (JTF-CND). Their primary focus, "…coordinating and directing the defense of DoD computer systems and computer networks," was ensuring the integrity and availability of those networks and keeping potential adversaries out [16].

With the OPTN structure still relatively new, the Air Force sought to beef up their approach to defending its networks by integrating more robust and dynamic network defense systems into them. Firewalls, proxy servers, and intrusion detection systems all became common place in network control centers around the world. However, dissimilar systems were surfacing which caused configuration management problems and ultimately weakened the overall security. The lack of centralized funding caused major commands and individual bases to fend for themselves with end-of-year monies to procure as much defense as they could. However, in 2000 the Air Force formalized their stance on network defense by directing the standardize purchase and installation of the Network Management System-Base Information Protection suite of hardware and software [17]. Although funding was still sparse, this step showed the Air Force was making an earnest effort to address the issue of defending the precious nature of information systems.

In addition to targeting the multitude of management and security issues associated with running networks, the OPTN effort discovered training to be a significant hurdle. Training was, and still is, one of the greatest challenges facing Air Force leaders

as they attempt to get networks operating as weapons systems. OPTN created a network operations crew structure with specific duties to emulate the aircrew system seen in aircraft and operations centers. These crews would man the base-level network control centers and major command network operations and security centers with several positions created specifically for network defense, such as boundary protection and intrusion detection. Career field managers for the communications and information career fields began adding network defense training in enlisted 5-, and 7-skill level technical schools to prepare them for their new crew-oriented duties. While the basic courses addressed boundary protection and intrusion detection, advanced courses covered topics such as reconnaissance, malicious logic, and the insider threat [18]. Communications and information officers were also receiving the basics in network warfare, information operations, security and availability in their initial and mid-level training schools, further showing the Air Force's emphasis on the importance of properly defending their networks [19].

A Shift Toward Offensive Operations

However, for nearly a decade, the Air Force and DoD have seen a shift in strategy to include offensive information operations. Lessons learned from the exploits of information and information systems during Operation DESERT STORM had already led the Air Force to create the Air Force Information Warfare Center (AFIWC). Although its mission did not initially include offensive operations, the creation of the AFIWC signaled an awareness that the Air Force saw the direction of future warfare. Several year later however, the AFIWC roles did shift to be the Air Force lead for developing tactics and

training for offensive and defensive counterinformation [20]. But, the Air Force's *Global Engagement* document, created in 1996, included Information Superiority as a new core competency for the Air Force. It defined Information Superiority to be "…the capability to collect, process, analyze and disseminate information while denying an adversary's ability to do the same." The definition alone implies an offensive capability when it talks of "…denying an adversary's ability to do the same." And the document goes on to state "The Air Force will aggressively expand its efforts in defensive IW as it continues to develop its offensive IW capabilities" [21]. The Air Force went on to formalize the inclusion of Information Operations in the spectrum of future warfare by creating Air Force Doctrine Document (AFDD) 2-5, *Information Operations*, in 1998. In it is stated: "The Air Force believes information operations include actions taken to gain, exploit, defend, or attack information and information systems." Had there previously been any doubt about Air Force views of offensive information operations, AFDD 2-5 made them clear [22]. Yet another signal that the times were changing was when the joint services organization responsible for command and control warfare (C2W), the Joint Command and Control Warfare Center, was redesignated the Joint Information Operations Center in 1999. C2W is "The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities…" [23], in which there is no mention of offensive information operations. However, their new mission is now the integration of Information Operations (IO) into military plans and operations across the spectrum of conflict, where IO is defined as "…actions taken to affect adversary information and

information systems while defending one's own…" This signaled the inclusion of IO tactics and capabilities into Joint operational war plans [24]. Equally significant, the JTF-CND was also redesignated as the JTF for Computer Network Operations in 2001 and was explicitly given the new mission of Computer Network Attack (CNA) [25]. Where their previous mission was exclusively "…defense of DoD computer systems and computer networks…" [26], it explicitly stated "The CNA mission is to coordinate, support and conduct, at the direction of the president, computer network attack operations in support of regional and national objectives." The Air Force continued its refinement of information operations and continues to show an increasing trend toward offensive operations. In February 2004, the Air Force published the *Concept of Operations for Information Operations* (IO CONOPS). In it, the CONOPS specifically addresses network attack operations (NetA) as a capability for future combat operations which would be integrated into existing conventional planning. NetA is defined in the CONOPS as "…the employment of network-based capabilities to destroy, disrupt, corrupt or usurp information resident in or transiting through networks" [27]. Additionally, AFDD 2-5, is in its final rounds of coordination and also includes network attack as an integral part of the Air Force's mission.

What appears to be missing from this clear shift in offensive operations is any mention of who will implement them. The Air Force is structured in a way that offensive weapons are employed by officers flying weapons systems. This project continues that premise and creates a career force development model to produce qualified officers to employ offensive information weapons.

III. Methodology

Overview

Having provided background into vulnerabilities from America's dependence on information and information systems, and the potential threat of future information warfare, the next logical step may very well be determining how the Air Force creates the cyber warrior force needed to defend and fight those potential cyber wars. But before that question can be answered, it's necessary to familiarize the reader with the methodology and terminology used in the development of this report. Although this research effort is not based on the results of laboratory experimentation, the same structured methods used to develop a well organized experiment are applied here as well. To assist in this development, the structured approach identified by Raj Jain in his book, *The Art of Computer Systems Performance Analysis* [28] is followed. If implemented, this approach will aid in determining the effectiveness of the model and the factors applied during implementation.

Goal

The goals of this project are to develop and document a proposed model for officer career development and progression within Information Operations, specifically, Network Warfare Operations (NW Ops). This model includes recommendations for education, training, experience and assignment types, all necessary components for producing a qualified Air Force cyber warrior force. This model can be used to support future offensive network attack operations.

Approach

The approach used to produce this NW Ops professional development model includes the analysis of other career field progression models. Specifically, the specialty fields of acquisition, medical, space operations and rated operations are examined in order to ensure any recommendations for the NW Ops workforce made are consistent with proven mainstream Air Force processes. Although the development of an NW Ops career force may be a new proposal, this approach does not depart from established processes. Based on these analyses, a solution is recommended for developing Air Force NW Ops personnel from accession through senior leader positions. The author is keenly aware of the significant challenges associated with changes in a system as large and complex as that of the Air Force, to include the substantial investment required to adopt these changes. However, due to the scope of this project, it is difficult to address in sufficient detail all the resource requirements, whether personnel or finances, needed to implement any potential recommendations made here.

System Boundaries

With the goals and the approach stated, it's important to define the scope of the model. In this project, it is initially tempting to define the boundaries of the system under test as the Air Force in its entirety, since the Air Force has the ultimate effect on the success or failure of this effort. However, that definition quickly becomes unwieldy as one tries to determine how to manage all the many facets of the Air Force. It was also tempting to limit the system to only the individuals who may pursue the NW Ops career force. But that proved too limiting when analyzing the parameters which affect them.

Based on that, the definition for the system defined by this project is the elements of the Air Force which have a significant effect on the individuals, namely the personnel system, assignment system, training system, and the organizations cyber warriors are assigned as reflected in Figure 1. Using the model which Jain defines as a system, that leaves the individual as the component under study or test.

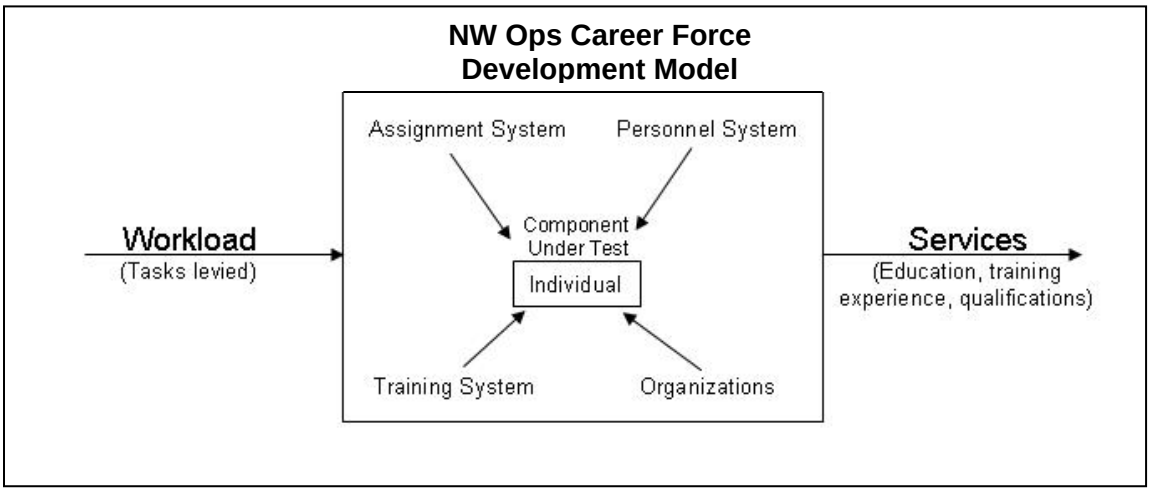

Figure 1 – System Boundaries

System Services

Regardless of how a system is defined, each system provides one or more services which a user can request. The same holds true for this research effort. Having established the system as the individual and the elements of the Air Force which directly affect them, the services generated by the component under test, the individual, are of greatest interest. The services generated by them are simply the education, training, experience, and qualifications of the individual which make them capable of defending Air Force, or DoD networks, or attacking those of their adversaries as necessary.

Workload

In general, the workload for a system is defined as a list of service requests. For the system identified in this report, workload is the demands placed on the individual as they progress through the career force process. These demands include education and training demands during periods of qualification, and various tasks levied upon them to demonstrate their proficiency or execute network defensive or offensive actions.

Performance Metrics

Performance is a key criterion in the design of any system. Performance is also key to the system and the processes ultimately proposed in this report. With the component under test identified as the individual, performance measures must be created to determine the success of individuals as they progress through their careers. Several metrics could potentially measure that success, but for the purposes of this effort, those listed below are used.

- Time required to meet qualification standards for assigned special experience identifier (SEI). Unit of measure: months per SEI (categorized by SEI)
- Number and types of SEI obtained. Unit of measure: SEI(s) obtained (based on final SEI categories)
- Successful completion of assigned training or education. Unit of measure: Training/education module pass rate (ratio of successful modules / modules attempted)
- Successful completion of incremental performance measures (e.g. checkrides, exams, etc.) Unit of measure: Check ride or exam pass rate (ratio of successful check rides or exams / check rides or exams attempted)
- Successful career progression (rank attained before separation) Unit of measure: Categorical unit of final rank attained
- On-time promotion success. Unit of measure: On-time promotion rate (ratio of on-time promotions / promotion boards met)

System Parameters

Parameters are defined as characteristics which affect the performance of the system. Parameters can either be system parameters, which directly apply to the system, or workload parameters, which vary the workloads. Although not an all-inclusive list, system parameter which could possibly affect the performance of the individual include:

- Previous experience. The experience an individual has upon entering the NW Ops career force can have a significant effect on their success. Whether obtained from a former career field or through personal study and experience, those skills could enhance their ability to learn additional skills or progress through their training or assigned tasks.
- The Air Force Assignment System. Aligning the individual with proper assignment which will afford them the opportunity to train and develop their skills will certainly affect their success.
- The Air Force Personnel and Finance Systems. Overall, the Air Force Personnel System has a significant affect on the potential success of an individual. In addition to assignments, other programs, to include pay, allowances, and incentives, which in turn affect the morale of the individual (whether financial or not) can affect the success of their career.
- Supervisors. Supervisors can also affect the success of an individual. If not appreciated, or recognized for their efforts, individuals can easily become disenchanted with the Air Force which in turn could affect their success. Also, supervisors have a great deal of control over training allocations and other opportunities which may impact the success of an individual.
- Air Force Budget. Changes in the Air Force budget can affect the training dollars, equipment, systems, etc., available at the unit level which can ultimately affect an individual's success.
- Deployments. Similar to assignments, deployment opportunities can have both positive and negative affects on an individual and in turn potentially impact their success.
- Training and education demands. Coursework, performance evaluations, and examinations are all items which can clearly affect the success of the individual. The intensity or frequency of these can ultimately determine an individual's ability to perform.

Workload Parameters

Since workloads for this project are the service requests levied on the individual, changes in those demands can clearly affect the success of the individual. Workload parameters include:

- Educational requirements
- Training demands
- Evaluations
- Examinations
- Performance tasks

However, when considering the definition of the system and component under test, it tends to lend itself to the performance tasks as being the only real demand placed on the individuals. Since the personnel, assignment, and training systems are all part of the larger system under test, the other parameters above are better suited as system parameters and are included there.

Factors

As with parameters, factors are also characteristics which affect the performance of the system. Factors are essentially the subset of parameters which are varied in order to see the resulting outcomes. If the recommendations of this report are implemented, factors need to be identified in order to see the impact on the process and its individuals. The factors the author feels would be the most applicable to the system and processes proposed in this report are Previous Experience and Training/Education demands. Since the NW Ops career force manning will initially come from existing career fields, it would be worth studying to see how well the various individuals in various positions succeed based on their backgrounds. Additionally, it would be worth determining how much

education and training the individuals need to perform the tasks levied upon them as requirements of the cyber warrior force are better defined.

Evaluation Technique

The evaluation technique is the method or methods in which the system is tested to accomplish the goals of the experiment. Techniques include mathematical modeling, computer simulations, and direct measurement. The selection of the right technique depends on the time and resources available to measure it. The most appropriate evaluation technique for this model would be direct measure. Unfortunately in this project, the timeframe needed to collect many of those metrics will span several years. It may be possible to generate a computer simulation which could predict some aspects of these processes, but that would have to be addressed in a separate study.

Experimental Design

Using direct measurements as the technique, this experiment produces a succinct design which minimizes the complexity. In many experiments, there are multiple factors, and multiple levels of each, which can be varied to perform the experiment. The typical experiment is done in two phases, where in the initial phase multiple factors are tested, but with a small number of levels. In the second phase, a subset of factors are tested, but at increased levels. In this project, there are only two factors recommended, which facilitates the execution of it. However, considering the multitude of options for the education and training factor, it's possible to scope a more complex experiment if additional considerations need to be addressed.

Likely candidates for inclusion in the cyber warrior force, include Communications and Information personnel, Intelligence personnel, Engineers, and possibly others. Considering those career fields, a reasonable division of backgrounds or previous experience, may very well be the Communications and Information career field (33Sx), compared with all others. Likewise, another possible division of previous experience may be those with technical undergraduate degrees, compared with those without (provided individuals are selected who didn't complete technical undergraduate programs). This report is advocating that all individuals considered for the cyber warrior force complete technical undergraduate programs, but determining their success with or without one may be a useful result of this experiment. This report proposes to arrange the experiment based on varying the previous experience category by previous career field, and undergraduate program. Additionally, this report proposes to vary the education and training factor by adjusting the amount of network and security fundaments offered. Individuals with backgrounds in networking or security may be successful without reaccomplishing those areas.

Below is a simple matrix that shows proposed combinations of factors to scope the experiment.

Table 1 - Experiment Design

Previous experience	**Completed network and security education and training.**	**Bypassed network and security education and training.**
Comm and Info (33Sx)		
With technical undergraduate degree		
Without technical undergraduate degree		
All Other career fields		
With technical undergraduate degree		
Without technical undergraduate degree		

Analyzing and Interpreting Results

Upon completion of the experimental data collection of the performance metrics above, this project proposes an analysis on the factors to determine the effects caused by each. The analysis will use a full-factoral design to determine if there is any significant difference in the success of individuals, using the categories matrixed in table 1. The effects will be analyzed for their significance and interactions. These results will allow career field managers to tailor the education and training tracks to produce the most effective system to produce cyber warriors

IV. Analysis

Creating The Force

The next step to consider is how the Air Force should proceed to create a cyber warrior force. It must be stated at this point that a great deal of effort across the Air Force has been directed toward the development of an information operations career force. In March of 2003, the Air Force approved the Information Operations Strategic Plan which was created to "…increase IO capability and effectiveness through a combination of doctrinal, programmatic, and organizational improvements" [29]. Additionally, the Air Force created the IO Implementation plan, "…to provide a process to integrate IO capabilities and provide the warfighter with a viable means to achieve non-kinetic effects" [30]. A key aspect of the plan was the creation of the Information Operations Steering Group (IOSG). The IOSG oversees the myriad of issues dealing with information operations, to include the task of creating an IO career force. The IO Strategic Plan, based on direction from Defense Planning Guidance 04-09 (DPG 04-09), directed the IOSG to develop an Air Force IO career force [31] . DPG 04-09 directed all component services to create a professional IO force, but did not specify details on how it was to be done. Although the IOSG will address the IO career force in its entirety, covering electronic warfare operations, network warfare operations, and influence operations, the scope of this project will only address network warfare operations, specifically network defense (NetD) and network attack (NetA).

Personnel System Issues

The efforts of IOSG have not only wrestled with what the professional development requirements for a new IO career force should be, but also those of the personnel system in order to manage newly trained IO career force professionals. One important point from the IO steering group efforts is that they advocate what could be considered as *part-time* IO professionals who will move in and out of IO billets rather than remaining in them through their career [32]. Additionally, the IO roadmap also recommends that personnel identified to work information operations receive tours that would alternate them between information operations jobs and those of their traditional career field [33]. However, others advocate an entirely different shift in perspective, that of a truly professional full-time information operations force. Through his research on this subject at Air Command and Staff College (ACSC), Major Jonathan Sutherland concluded about the part-time IO approach, "Sending a college graduate to the field for a few tours of general expertise interspersed with training classes and then expecting first-rate information techniques in a more specialized tour later is not adequate" [34]

The development of a truly professional force is essential to ensuring these individuals receive the training, assignments, and leadership opportunities to be successful in their careers. Those advocates recommend this be done by the creation of a new Air Force Specialty Code (AFSC) which would completely identify them as a separate career field. However, the IOSG maintains that individuals will remain in their existing AFSC but receive a Special Experience Identifier (SEI) as a means to identify the specialized IO experience they've gained. Regardless of whether a new AFSC is created or not, this report advocates that individuals be trained, tracked, and managed as

information operations professionals, and that they not be rotated or alternated through assignments, or ever be considered *part-time*.

Determining Force Size

One thing that may be agreed upon is that irrespective of how the individuals are coded and tracked, there will likely be no new forces to access into the IO career force. According to the Air Force Chief of Staff, "By the end of 2005, we should reduce the size of our active force by 16,000 people…" [35]. Consequently, all individuals identified to be IO career course professionals will undoubtedly come from existing forces. Naturally there may be some hesitation among career field managers to release individuals from their existing career fields to populate this new IO force. Unfortunately, the reality may be that if the Air Force wants to ensure a truly professional force, that's a level of pain that needs to be endured.

A difficult step in making that happen is determining the exact numbers to populate the career force with. Typically the Air Force mans specialties based on specific organizational requirements or by inventory (based on a specified percentage of the force) [36]. To facilitate the management of the new NW Ops career force, this report recommends an inventory-based approach until the NW Ops career force has the opportunity to mature and potentially drive more refined requirements. Likely sources or career fields to draw from would be the communications and information career field, intelligence career fields, or engineering career fields. However there are undoubtedly individuals in a multitude of career fields who possess the fundamental skills or educational background to easily transition into the information operations career force

area. One possibly approach may be to survey the Air Force to find these individuals.

Regardless of the source, a key to successful development of the NW Ops career force will be the correct balance of education, training, assignments, and job experience.

> The information warrior must know not only programming but systems integration and systems theory, communications, security, artificial intelligence, logic in all its many forms (classical, fuzzy, and convergent), and statistical techniques. The information warrior must also know the customer's needs: the commander's intent, doctrine, and strategy. The amount of information necessary to be an information warrior is immense, and the time required to master it would have to be at the expense of a more general command instruction. [37]

Referencing Other Career Field Models

Acquisition

The right balance of these areas is certainly not new to the Air Force, nor other career fields. For example, the acquisition community has categorized all positions and all assignments by certification level. They've done this in an effort to ensure that only fully trained and qualified personnel occupy those critical billets. They've also included the prerequisite education requirements to fill those assignments and the job experience requirements to gain additional certifications if necessary to remain in them. They have well-established courses all individuals must attend at various levels which prepare them for the job responsibilities commensurate with those certification levels. Senior leaders in the acquisition community must not only meet the highest level of certification, but they have additional statutory requirements that must be met [38].

Medical corps

In the medical corps, they too have a multitude of educational and job requirements to ensure their force is professionally trained and qualified. In addition to

the minimum education requirements of medical school, they must complete a minimum of one year of graduate training and examinations in order to obtain a medical license for the state in which they practice. Beyond that, they need an additional three years of training to be a fully qualified doctor. In addition to clinical experience, they are required to complete approximately 50 hours of continuing education units per year just to maintain their state license. As they advance through their career and attain advanced specialties, they may complete board certifications for those added specialties. With each certification comes a list of criteria they must meet in order to retain them. In addition to state and board certification requirements, each clinic or hospital may specify skills requirements specific to their facility and position. Proficiency is maintained through the numbers and types of procedures they complete in clinical practice, and the arduous peer and senior staff review process they participate in. Lastly, advanced education is strongly emphasized as well. At any point in time, there are approximately 25 percent of all doctors in graduate education programs [39].

Space Operations

An interesting development in the space operations career field recently is the establishment of a space warrior cadre. The 2001 Space Commission contended Air Force and DoD Space Operations personnel were not adequately trained or educated and "…are not yet on course to develop the space cadre the nation needs." As a result, the space operations career field is undergoing a change in how they train, educate, and manage their space professionals. Similar in design to that of the acquisition career field model, all space operations billets will be reviewed and identified for required experience and certification levels to work them. They too will create a three-tiered certification

system in which individuals will progress from accession through senior leadership positions. At each level, will be a mandatory course which will provide them the necessary education to fill assignments at that level. And similar to how the IOSG has advocated special experience identifiers to track IO career force professionals, they will create specialty codes, or *specs*, in order to manage individuals based on the various specialties that they attained [40].

Rated Operations

Lastly, in looking at the rated operations career field, one sees what may understandably be the most stringent technical training requirement in terms of war fighting proficiency skills. Each pilot completes undergraduate pilot training which qualifies them for initial training into their weapon system. At their weapon system entry school, they receive initial qualification training (IQT) where they learn the systems and operations, to include all facets of emergencies. This training entails many hours of both simulator and aircraft flying time. They complete numerous check rides which combine both open and close book examinations, covering both normal and emergency procedures. This rigorous training ensures pilots are proficient in the critical skills necessary to execute their duties in a wartime environment. At their first duty station, they proceed through mission qualification training (MQT) where they develop the proficiency to fly the aircraft through all facets of its designed capabilities and to employ all the weapons systems equipped on that aircraft. They are also required to maintain currency by flying a pre-determined number of hour in training sorties which are representative of the mission of the aircraft and its weapons systems. The next steps in their career are potentially those of advanced flying positions to include aircraft

commander, for multi-pilot systems, instructor pilot, or evaluator. The best of the best have the opportunity to go on to the Air Force Weapons School and become experts in weapons employment [41, 42].

Assessment and Recommendations

Having assessed a variety of career fields and their processes for developing their professionals, this report recommends one for the network warfare operations specialists. This recommendation essentially combines many of the key elements from those above. As with all the career fields, it includes timely training and educational opportunities at key points in an individual's progression to ensure their knowledge and skills are commensurate with the level of assignments they'll hold. Specifically, it includes an initial NW Ops course to offer both the theoretical and practical fundamentals of NW Ops which individuals will need to step into their first assignment. Additionally, this recommendation includes check rides and annual standardization examinations, as used by the rated operations career field, to ensure individuals are able to perform the tasks they have been deemed qualified to perform or to employ the weapons they are qualified to employ. Lastly, it also includes the requirement to complete continuing education units, like the medical career field, to ensure they remain current since the pace of technology change is so rapid.

NW Ops Officer Requirements

The first step in the development of the NW Ops career force is to determine, as much as possible, the requirements individuals will need to execute the mission of

network defense or attack, and thus to be successful in their careers. Joint Publication 3-13 identifies the following as expectations of IO professionals [43].

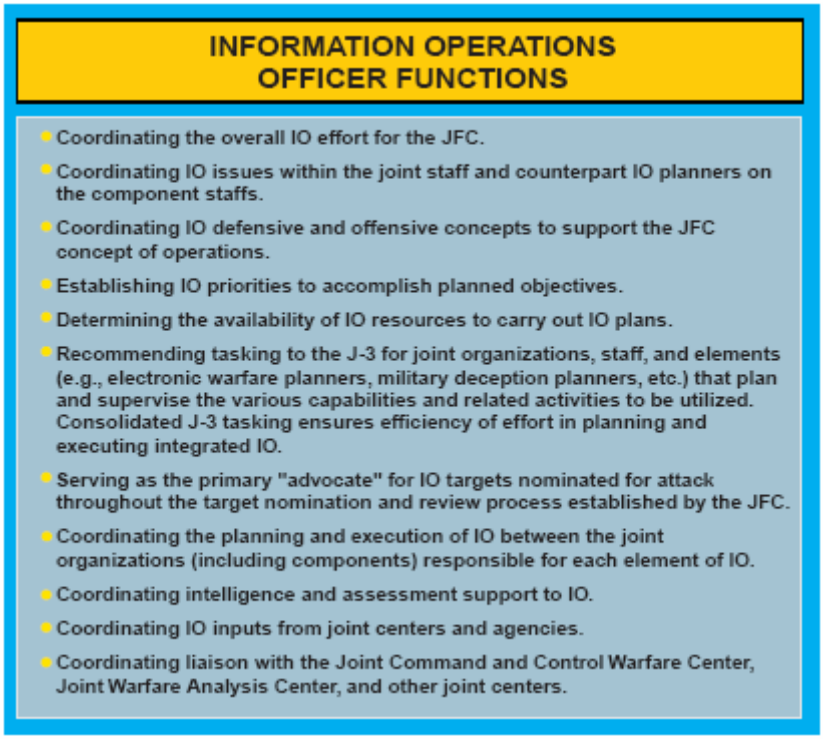

Figure 2 – IO Officer Functions

These requirements are levied on all IO professionals regardless of specialty. Clearly, they focus very heavily on the roles of planning, execution and support to a joint forces commander (JFC). It seems evident that the training and experience necessary to be effective at that level is extensive. Additionally, the DoD IO Roadmap further identify the types of knowledge and skills the individuals must possess by stating, “IO capability specialists should possess specialized expertise on a certain IO core capability, but gain experience in the planning and execution of the broader construct of IO” [44]. Based on

these expectations, this report attempts to identify the education, training, and experience requirements for NW Ops professionals to perform at these levels.

Undergraduate Requirements

Prior to their acceptance in the NW Ops career force, potential candidates should have a technical undergraduate degree. It's not essential that they complete an engineering or computer science degree, but it's important that their undergraduate program be technical in nature, and includes several engineering or computer science courses. This technical undergraduate program will aid the individual in their completion of the initial NW Ops course.

Initial NW Ops Course

To begin the pursuit of the NetD and NetA specialties, individuals must understand the fundamentals of the environment and technologies in which they work. This is accomplished through a rigorous course, or courses, which provide the foundation upon which the NW Ops specialists will build. Although HQ ACC/SCN is working on potential course requirements, this report includes recommendations on the subject matter the courses need to address. Table 2 outlines the course content for the initial NW Ops course.

Table 2 – Initial NW Ops Course Content

Initial Network Warfare Operations Course Material Content
Fundamentals of Information Warfare (IW)
AFDD 2-5
Information Operations (IO)
Influence Operations (Influence Ops)
Electronic Warfare Operations (EW Ops)
Network Warfare Operations (NW Ops)
Legal/Ethical Aspects of IO/IW
Terrorism/Antiterrorism
C4ISR
Space Systems
Air Operations Center (AOC) Operations
Operational Campaign Planning
Operations Security (OPSEC)
Fundamentals of Network Operations
Network Operating Systems
Network Management Principles
Network Infrastructure Devices
Networking Protocols
Air Force Enterprise Networking
IO/IW Threats, Vulnerabilities, Methodologies, and TTPs
Emission Security (EMSEC)
Communications Security (COMSEC)
Computer Security (COMPUSEC)
Security Management
Access Control Models
Social Engineering
Operating Systems Fundamentals and Vulnerabilities
Software Vulnerabilities
Distributed System Security
Secure Application Development
Malicious Logic and Scripting
Telephones System Vulnerabilities
Infrastructure Devices and Vulnerabilites
Wireless Technologies and Vulnerabilities
Data Integrity
Encryption
Network/computer Forensics
Firewalls
Proxy Servers
Intrusion Detection Systems
VPNs

Completion of the NW Ops course is a critical lead into the NW Ops career force. Clearly the scope of the material covers all aspects of IO to ensure individuals understand the broader IO discipline. Later in their NW Ops career, individuals will have the

opportunity to attend the intermediate NW Ops course where the emphasis will concentrate more on IO planning. However, during the initial NW Ops course, individuals will concentrate more on the technical aspects of NW Ops, addressing only the fundamental elements of EW Ops and Influence Ops. The initial NW Ops course will offer sufficient depth into networks, network security, and the elements of NW Ops necessary for individuals to be prepared for the demands placed on them upon graduation. It will include adequate hands-on training with standard Air Force equipment, systems, and applications so individuals will easily transition into the operation of live networks at their next assignment.

Career Path

The initial NW Ops course is simply the first step in a long progression of assignments and training opportunities which ultimately leads to a qualified and proficient NW Ops career force. Not all individuals will follow the same path, nor will all individuals attain the same levels of rank or career success. Although there is no set track an individual must follow, there are elements of assignments which will allow individuals the opportunity to be successful. Below are templates for assignment types and levels which individuals should attempt to follow to become successful NW Ops specialists.

First Assignment

Upon completion of the initial NW Ops course, personnel report to their first duty location. Table 3 lists typical assignment types that individuals should receive for their first assignment out of the initial course.

They will receive additional education and training to learn the specific mission of their unit and parent major command, and at that point are considered *initially qualified* and enter mission qualification training (MQT). MQT will entail qualifying for one of the special experience identifiers in the network control center NetD positions. That qualification will include several check rides and examinations with certified evaluators.

Table 3 - Typical NW Ops First Assignments

Typical First Assignments	**Performance Requirements**
Base Network Control Centers (NCC)	Systems and emergency procedures checkout (IQT)
Combat Communications Squadrons	MQT – gain NCC NetD position qualification and SEI
Other Communications and Information Officer Aerospace Communications Education billets	Qualification and annual checkrides
	Annual standardization and emergency procedures exams
	Currency through CEUs

Also at their first assignment, they need to acquire continuing education units to ensure they remain current and knowledgeable on trends and technologies relevant to network warfare issues. Qualified individuals will demonstrate their proficiency at least annually through performance checkrides and annual standardization examinations.

Second Assignment

Upon reaching their second assignment, individuals will again be required to complete local check rides that will cover emergency procedures in addition to organizational and major command mission specifics tasks. Table 4 lists typical assignment types that individuals should be considered for as second assignments.

Table 4 - Typical NW Ops Second Assignments

Typical Second Assignments	Performance Requirements
Network Operations and Security Centers (NOSC)	Systems and emergency procedures checkout
Information Warfare Flights (IWF), Information Warfare Squadrons (IWS), Information Warfare Aggressor Squadrons (IWAS)	Gain additional NetD/NetS position qualifications and SEIs
Air Force Network Operations and Security Centers (AFNOSC)	Learn offensive network operations TTPs
Air Force Computer Emergency Response Team (AFCERT)	Upgrade to instructor or evaluator
Battle Labs	Participate in operational exercises (e.g. Red/Blue Flag, Black Demon, etc.)
	Qualification and annual checkrides
	Annual standardization and emergency procedures exams
	Currency through CEUs

Their second assignment may include earning additional special experience identifiers in any of the network defense or network support categories, or they may begin to learn and practice offensive network tactics techniques and procedures. Based on the rate at which they're able to progress, they may also begin to qualify as trainers or evaluators. This would also be a prime opportunity for individuals to look to participate in operational exercises, such as Red or Blue Flags or Black Demon, that would allow them to apply the knowledge and skills they have gained. During this assignment, they will again be subjected to multiple check rides, including annual examinations, to ensure they maintain their skills and proficiency. They will also complete the required continuing education units to ensure they remain current with network warfare technologies and vulnerabilities.

Third Assignment

The third assignment offers qualified personnel opportunities to possibly branch out and explore other areas of network warfare operations. Table 5 lists typical assignment types that individuals should be considered for as third assignments.

Table 5 - Typical NW Ops Third Assignments

Typical Third Assignments	Performance Requirements
Competitive programs like SOS, EWI, AFIP, AFIT	Emergency procedures checkout
Executive Officer	Gain additional NetD/NetS position qualifications and SEIs as applicable
Staff action officer or IO planner (MAJCOM, NAF, DRU, FOA levels)	Qualification and annual checkrides
Instructor duty: Initial NW Ops course	Upgrade to evaluator or developer of TTPs
Intermediate NW Ops Course student	Participate in operational exercises (e.g. Red/Blue Flag, Black Demon, etc.)
Air Operations Center Course student	Annual standardization and emergency procedures exams
Air Force Weapons School student	Currency through CEUs
	Staff IO planner

They may be afforded the opportunity to attend Squadron Officer School in-residence, or programs like Education With Industry (EWI), the Air Force Intern Program, and the Air Force Institute of Technology. They may also have the opportunity to serve as an executive officer, or in other highly selective positions. Timing would also put them in the window to gain additional training in the Intermediate Network Warfare Operations Course, Air Force Weapons School, Air Operations Center Course, or other courses such as those at the Joint Special Operations University [45]. Depending on their proficiency and rate of progression, they may be given the opportunity for assignment as a school house instructor at the initial NW Ops course. Toward the end of the third assignment they may transition into an IO planning function if co-located with a Numbered Air Force (NAF) or Major Command (MAJCOM) Headquarters. Again, they should take every opportunity available to participate in operational exercises to reinforce their skills and tactics, techniques, and procedures (TTPs). They may also participate with, or on, staff entities as evaluators or developers of the TTPs that network warfare operations personnel use. As qualified NW Ops specialists, they will again be expected

to complete continuing education units, annual standardization examinations, and checkrides.

Intermediate NW Ops Course

After their first two or three assignments, NW Ops professionals should have the opportunity to attend the Intermediate NW Ops Course. This course will build on the material taught in the Initial NW Ops Course and the experience individuals gain in their early assignments. The course will offer advanced offensive NW Ops TTPs, and will emphasize IO planning, to include all aspects of IO. As individuals become more senior, this course will assist them in their transition to IO planning assignments. Table 6 outlines the recommended course content for the Intermediate Network Warfare Operations Course.

Fourth Assignment

The fourth assignment will offer many similar opportunities as those of the third assignment, depending on what individuals have done to this point in their career. Table 7 lists typical assignment types that individuals should be considered for as fourth assignments.

Table 6 – Intermediate NW Ops Course Content

Intermediate Network Warfare Operations Course Material Content
Terrorism/Antiterrorism Intelligence Update
Current Trends in IO/IW Threats, Vulnerabilities, Methodologies, and TTPs
AFDD 2-5
Legal/Ethical Aspects of IO/IW
Advanced Concepts in Information Operations (IO)
Air Operations Center (AOC) Operations
Operational Campaign Planning
Offensive NW Ops TTPs
IO Planning and Execution
Influence Operations (Influence Ops)
Electronic Warfare Operations (EW Ops)
Network Warfare Operations (NW Ops)

Table 7 - Typical NW Ops Fourth Assignments

Typical Fourth Assignments	Performance Requirements
Many of the same types as for third assignments, plus:	Currency through CEUs
Flight Commander	Staff IO planner
Highly selective programs like IDE, EWI	Upgrade to evaluator or developer of TTPs
IO planner (NAF/MAJCOM/HAF/Joint HQs levels)	

As more senior members, they may have the opportunity to fill key leadership billets such as flight commander. Additionally, they may have the opportunity to attend Intermediate Developmental Education (IDE) opportunities such as ACSC, the Air Force Institute of Technology or the Naval Postgraduate School. This is also the right time to look toward participation on NAF, MAJCOM, HQ Air Force (HAF), or Joint Headquarters staffs to perform IO planning and staff functions.

Fifth Assignment

The fifth assignment will be an even more senior assignment that may include IDE, instructor duty, at either the Initial or Intermediate NW Ops courses, or Air Force weapons school, or such typical jobs as an IO planner or staff member at various Agency, HAF or Joint Headquarters levels. They may also be able to attend additional courses such as the Senior Information Warfare Applications Course [46].

Subsequent Assignments

Their sixth and subsequent assignment opportunities are increasingly more senior and take on additional leadership roles and responsibilities. These may provide the opportunity to compete for squadron command, or attend Senior Developmental Education opportunities, the Joint Information Warfare Senior Officers Course at the National Defense University, or participate as the senior staff member involved in IO

doctrine at MAJCOM, HAF or Joint Headquarters levels. Individuals at this point in their careers should be looked upon as the senior experts in all aspects of IO, not only NW Ops. Figure 3 shows a notional career planning diagram for Network Warfare Operations specialties.

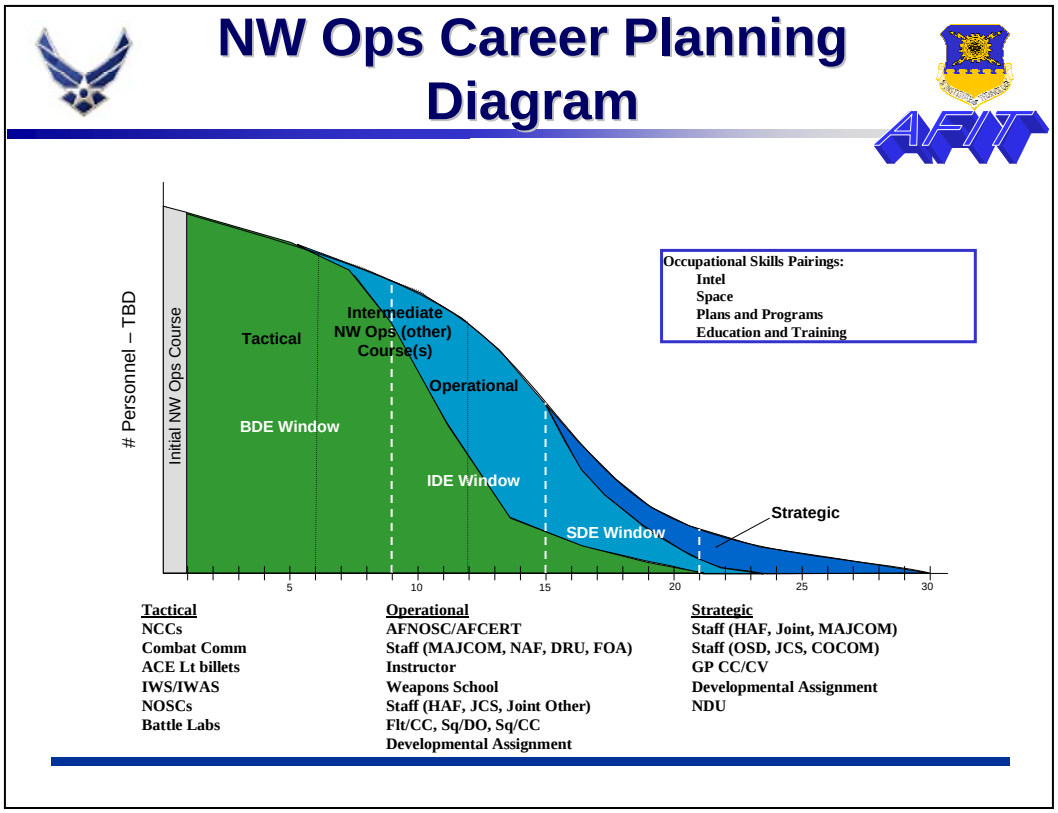

Figure 3 – Network Warfare Operations (NW Ops) Career Planning Diagram

V. Conclusion

Several senior military leaders and strategists have supported the idea that future information warfare is a distinct possibility. The threat exists not only by nation states, but also by non-nation terrorist organizations, and has been substantiated by national security and international terrorism experts. For nearly ten years, the Air Force and DoD have written IO concepts into key documents acknowledging the potential of future IW. For most of that decade, the Air Force and DOD have focused on a defensive posture to protect themselves from the potential of an information warfare attack. However, there has been a clear shift in philosophy which includes integrating offensive information operations into operational doctrine and war plans. What appears to be lacking however, is the trained and qualified information operations force with the expertise to prosecute an information war or employ offensive information weapons. Last year, the Air Force activated the information operations steering group whose charter is to address the wide range of issues dealing with information operations to include the creation of an IO career force. Their efforts however, do not call for a separate IO force, but rather individuals from other specialties who receive IO training. Additionally, the IOSG advocates alternating assignments between an individual's original career track and IO billets. Having assessed several existing Air Force career fields, the recommendation from this report is to create a new NW Ops career force who specialize in IO activities for their entire career. This report also proposes a career development and progression model which outlines the types of assignments and performance expectations individuals should follow to produce a trained and qualified NW Ops career force.

Bibliography

1. Department of the Air Force. *Corners of Information Warfare*. Washington: HQ USAF, 1995.

2. Jumper, General John P., Commander, U.S. Air Forces in Europe. Defense Colloquium on Information Operations. March 1999

3. Department of the Air Force. *Concept of Operations for Information Operations*. Washington: HQ USAF, 2004.

4. Goldberg, Ivan M.D. Institute For The Advanced Study Of Information Warfare. http://www.psycom.net/iwar.1.html. 6 July 2004.

5. US Department of Commerce. "*The Emerging Digital Economy*: *Building Out the Internet*." http://www.ecommerce.gov/emerging/htm. May 1998

6. Internet Word Stats: Usage and Population Statistics. "Internet Usage in North America." http://www.internetworldstats.com/stats2.htm#north. July 2004

7. Henry, Ryan and C. Edward Peartree. "Military Theory and Information Warfare," *Parameters*. http://carlisle-www.army.mil/usawc/Parameters/98autumn/henry.htm. (Autumn 1998)

8. Craig, Captain (USN) D.W. *Asymmetrical Warfare and the Transnational Threat: Relearning the Lessons from Vietnam*. Advanced Military Studies Course, Canadian Forces College. http://198.231.69.12/papers/amsc1/006.html. September 1998

9. The Associated Press. U.S.: China reassessing its military strategy, Beijing has taken notice of U.S. military performance in Iraq. http://www.msnbc.msn.com/id/5103836/. May 31, 2004

10. Ancker, Clinton J., III and Michael D. Burke. Doctrine for Asymmetric Warfare. http://www.findarticles.com/p/articles/mi_m0PBZ/is_4_83/ai_109268858. July-August 2003

11. Clarke, Richard. "CyberWar." http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/clarke.html. Interview with PBS. March 18, 2003.

12. iDEFENSE Security Advisory 10.16.03. "Global Cyber Threat: Will Malaysia Emerge as a Pro-al Qaeda Cyber Terrorist Haven?" http://www.idefense.com/application/poi/display?id=68&type=global_threat&flashstatus=true. 2003

13. Department of the Air Force. *Concept of Operations for Information Operations*. Washington: HQ USAF, 2004.

14. HQ AFCIC/SY. "Operationalize & Professionalize The Networks - AF-Level Networking Roles & Responsibilities." Electronic Message. 1200Z 12 January 1998

15. CSAF. "Information Assurance--Protecting Our Networks." Electronic Message. 2138Z 27 October 1998

16. Lamb, Robert J. "Joint Task Force for Computer Network Defense." http://www.iwar.org.uk/infocon/dtic-ia/Vol2_No3.pdf. Winter 98/99, Vol 2, No. 3

17. HQ USAF/SC. "Network Management System/Base Information Protection (NMS/BIP), Standard Air Force System." Electronic Message. 2300Z 04 January 2000

18. Department of the Air Force. *AFSC 3C0X1 Communications-Computer Systems Operations*. CFETP 3C0X1. http://www.e-publishing.af.mil/pubfiles/af/cfetp/cfetp3c0x1/cfetp3c0x1.pdf. 1 October 2003

19. 333rd Training Squadron. "Expeditionary Communications Officer Training." https://etca.randolph.af.mil/showcourse.asp?as_course_id=E3OBR33S1%20%20%20011. February 2004

20. Air Force Information Warfare Center. "History." http://afiwcweb.lackland.af.mil/organization/history.cfm. 1999

21. Department of the Air Force. *Global Engagement: A Vision for the 21st Century Air Force*. http://www.au.af.mil/au/awc/awcgate/global/nuvis.htm. Washington: HQ USAF, 1996

22. Department of the Air Force. *Information Operations*. AFDD 2-5. Washington: HQ USAF, January 2002

23. National Communications System Technology and Standards Division. *Telecommunications: Glossary of Telecommunication Terms*. Federal Standard 1037C. http://www.its.bldrdoc.gov/fs-1037/dir-008/_1086.htm. Washington: General Services Administration Information Technology Service. August 1996

24. U.S. Strategic Command Public Affairs. "Fact File: Joint Information Operations Center." http://www.stratcom.mil/FactSheetshtml/Joint Info Operations Center.htm. March 2004

25. U.S. Strategic Command Public Affairs. "Fact File: Joint Task Force – Computer Network Operations." http://www.stratcom.mil/factsheetshtml/jtf-cno.htm. March 2004

26. Lamb, Robert J. "Joint Task Force for Computer Network Defense." http://www.iwar.org.uk/infocon/dtic-ia/Vol2_No3.pdf. Winter 98/99, Vol 2, No. 3

27. Department of the Air Force. *Concept of Operations for Information Operations*. Washington: HQ USAF, 2004.

28. Raj Jain. The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling. New York: John Wiley & Sons, Inc., 1991

29. Department of the Air Force. *Information Operations Strategic Plan FY04-09.* Washington: HQ USAF 2003

30. Department of the Air Force. *Air Force Implementation Plan, Information Operations: The New Warfare (Draft)*. Washington: HQ USAF 2004

31. Department of the Air Force. *Information Operations Strategic Plan FY04-09.* Washington: HQ USAF 2003

32. Department of the Air Force. AFMAN 36-2105 Update "Information Operations." Washington: HQ USAF/XOIW. 18 June 2004

33. Department of Defense. *Information Operations Roadmap.* Washington: OSD October 2003

34. Sutherland, Jonathan A. "Is it Time to Create an Information Operations Career Field?" Unpublished report. Air Command and Staff College, Maxwell AFB AL, 2004.

35. Jumper, General John P. *Chief's Sight Picture: Shaping the Force*. Washington: HQ USAF 2004. http://www.af.mil/media/viewpoints/shaping_force.html

36. Mercier, Mark. Chief, Force Mgmt Branch, Force Management, Plans and Policy Division, HQ USAF/ILCX, Washington. Telephone interview. 14 July 2004

37. Lubicki, Martin C. and James A. Hazlett, "Do We Need An Information Corps?" Joint Forces Quarterly, Autumn 1993

38. Department of the Air Force. "Acquisition Career Management: APDP Web Guide." http://www.safaq.hq.af.mil/acq_workf/career_training/apdp/certification_.html 2004

39. Nadeau, Mark T. Chief, Physician Education Branch, HQ AFPC/DPAME, San Antonio. Telephone interview. 21 July 2004

40. Commission to Assess United States National Security Space Management and Organization. *Space Commission Report (2001): Report of the Commission to Assess United States National Security Space Management and Organization*. Washington: January 2001

41. Davis, Harry A. Intermediate Developmental Education Student: Air Force Institute of Technology, AFIT/ENC, Dayton. Personal interview. 16 July 2004

42. Starr, Michael. Masters Student: Air Force Institute of Technology, AFIT/ENG, Dayton. Personal interview. 20 July 2004

43. Department of Defense. Joint Pub 3-13: Joint Doctrine for Information Operations. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf. Washington: October 1998

44. Department of Defense. *Information Operations Roadmap.* Washington: OSD October 2003

45. Joint Special Operations University. "Resident Course Offerings." https://www.hurlburt.af.mil/jsou/index.php. HQ USSOCOM. 2004

46. Air University. Senior Information Warfare Applications Course. http://www.cadre.maxwell.af.mil/warfarestudies/wsf/siwac.htm. Maxwell AFB: 2004

Vita

Born in Grand Island, Neb., Major Scott D. Tobin enlisted in the Air Force in 1980 and served as an aircraft maintenance technician until his selection into the Airman's Education and Commissioning Program. He graduated with honors from Wright State University, and in 1989 entered the officer corps through Officer Training School. His career combines various assignments as a communications systems engineer at unit, Major Command, and Air Staff levels, and was highlighted by tours in Southwest Asia, Europe, the Pacific, and most notably, Squadron Command.

Major Tobin was a student under the Intermediate Developmental Education program at the Air Force Institute of Technology (AFIT). Major Tobin's academic program was a Masters of Science in Electrical Science, specializing in Computer Networks and Information Assurance, through the Department of Electrical and Computer Engineering. Upon graduation from AFIT, Major Tobin will be assigned to the Defense Information Systems Agency, Arlington VA.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
14-09-2004	Master's Graduate Research Project	Mar 2004 – Sep 2004

4. TITLE AND SUBTITLE

ESTABLISHING A CYBER WARRIOR FORCE

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Tobin, Scott D., Major, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-8865

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GE/ENG/04-27

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Lt Col David Biros
AF-CIO/PO
1155 Air Force Pentagon
Washington D.C. 20330-1155

(703) 696-6317

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Cyber Warfare is widely touted to be the next generation of warfare. As America's reliance on automated systems and information technology increases, so too does the potential vulnerability to cyber attack. Nation and non-nation states are developing the capability to wage cyber warfare. Historically, the Air Force and DoD have concentrated their efforts toward defensive network operations. However, a shift in doctrine has shown both the Air Force and DoD acknowledging the potential for Information Warfare. What appears to be lacking is the trained and educated cyber warrior force who will carry out the information operations if needed. This research project examines the doctrine of DoD and national agencies to engage in information operations and efforts in place to train cyber warriors. In turn, this research project offers recommendations for a career development and progression model for an Air Force *Cyber Warrior* force.

15. SUBJECT TERMS

Cyber, Warrior, Networks, Information Operations, Career Progression

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Richard A. Raines, ENG
U	U	U	UU	52	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-6565, ext 4278 (richard.raines@afit.edu)